

無線區域網路之兼具效率與安全的數位典藏系統委任授權機制

張家証、曹偉駿

E-mail: 322093@mail.dyu.edu.tw

摘要

由於資訊科技的發展，無線網路逐漸成為多數國人之生活核心。另一方面，數位典藏計畫的推廣，長年已累積相當可觀的典藏資源，透過網路服務(Web Services)技術，於數位典藏資料庫與網站架構基礎上，提供整體服務如建立單一登入機制、內容使用之相互授權，實為一重要課題。在眾多網路服務存取控制策略當中，以角色為基礎的存取控制(Role-based Access Control, RBAC)機制與情境感知(Context-aware)元素加入，雖然可降低數位典藏系統管理員負擔，方便管理員檢視使用者權限，與提升系統穩定性。然而，隨著網路安全問題層出不窮，上述的存取控制機制是不足的。因此，本研究將補強「以角色為基礎的存取控制機制」與「情境感知」的安全性不足，改以「情境感知」結合至「委任授權」(Delegation)中，並支援於無線區域網路環境(wireless local area networks, WLAN)下，以便增進數位典藏系統效率及安全。此外，本研究並進一步開發系統雛型，以實際驗證所提之存取控制機制執行於無線環境的可行性，相信本研究成果若應用在無線數位典藏環境上，將除了有效減輕管理者負擔、提高用戶以無線方式使用典藏服務的方便性，同時亦提升典藏系統存取控制的安全性。

關鍵詞：數位典藏、無線區域網路、網路服務、角色為基礎的存取控制、情境感知、委任授權

目錄

中文摘要	iii	英文摘要	iv	致謝辭	v	內容目錄	vi	表目錄	ix	圖目錄	x	第一章 緒論	1																															
1 第一節 研究背景與動機	1	2 第二節 研究目的	2	3 第三節 研究流程	3	4 第四節 論文架構	4	第二章 文獻探討	6	6 第一節 無線數位典藏環境	6	6 第二節 存取控制機制之探討	11	11 第三章 建構無線網路使用者之兼具效率與安全的數位典藏委任授權機制	19	19 第一節 無線數位典藏環境之建構	20	20 第二節 具情境感知的委任授權機制	24	24 第四章 安全性與效益分析	31	31 第一節 安全性分析	32	32 第二節 效益分析	35	35 第三節 優勢分析	37	37 第五章 系統實作與成果展示	38	38 第一節 系統建置環境	38	38 第二節 系統部署與成果展示	39	39 第三節 成果討論	51	51 第六章 結論與未來展望	52	52 第一節 結論	52	52 第二節 未來展望	52	52 參考文獻	54	54

參考文獻

- 參考文獻 一、中文部分：古一浩(2006), Ajax 範例活用辭典, 台北:博碩文化。國立故宮博物院(2005), 如何數位典藏[線上資料], 來源: <http://tech2.npm.gov.tw/da/> [2010, June 10]。數位典藏國家型科技計畫 計畫網站(2010), 線上資料, 來源: <http://www.ndap.org.tw/> [2010, June 13]。蔡永橙, 黃國倫, 邱志義(2007), 數位典藏技術導論, 台北:中央研究院台大出版中心。二、英文部分：Abdallah AE. & Takabi H. (2010). Formalizing Delegation and Integrating It into Role-Based Access Control Models. *Journal of Information Assurance and Security*, (5), (pp. 021-030). Abdelzaher, T. F., Atkins, E. M., & Shin, K. G. (2000). Qos Negotiation in Real-Time Systems and its Application to Automated Flight Control. *IEEE Transactions on Computers*, 49(11), (pp. 1170-1183). Baru, C., & Rajasekar, A. (1998). A Hierarchical Access Control Scheme for Digital Libraries. *Proceedings of the Third ACM Conference on Digital Libraries* (pp. 275-276), United States of America: Pittsburgh. Cho, N., Lee M. & Gatton T. M. (2009). A Function-Based User Authority Delegation Model. *Information Sciences*, 180(5), (pp. 765-775). Coetzee, M. & Eloff, J. H. P. (2004). Towards Web Service Access Control. *Computers & Security*, 23(7), (pp. 559-570). Feigenbaum, J., Freedman, M. J., Sander, T., & Shostack, A. (2001). Privacy Engineering for Digital Rights Management Systems, *Proceedings of the ACM Workshop on Security and Privacy in Digital Rights Management* (pp. 76-105), United States of America: Pennsylvania. Ferraiolo, D., & Kuhn, R. (1992). Role-Based Access Control. *Proceedings of the Fifteenth NIST – NCSC National Computer Security Conference*. Ho, J. (2010). System and Method for Security Association between Communication Devices within a Wireless Personal and Local Area Network. United States Patent, No. 60/601, 402 Kapsalis, V., Hadellis, L., Karelis, D., & Koubias, S. (2006). A Dynamic Context-aware

Access Control Architecture for e-services. *Computers & Security*, 25(7), (pp. 507-521). Lu, E. J. & Chen Y. H., (2005). A Flexible Delegation Processor for Web-Based Information Systems. *Computer Standards & Interfaces*, 27(3), (pp. 241 – 256) Martin, F. J. P. (1999). Push vs. Pull in Web-Based Network Management. *Proceedings of Sixth IFIP/IEEE International Symposium on Integrated Network Management* (pp. 3-18), England: Boston. Strembeck, M., & Neumann, G. (2004). An Integrated Approach to Engineer and Enforce Context Constraints in RBAC Environments. *ACM Transactions on Information and System Security*, 7(3), (pp. 392-427). Tomur E. & Erten Y.M. (2006). Application of Temporal and Spatial Role Based Access Control in 802.11 Wireless Networks. *Computers & Security*, 25(6), (pp. 452-458). Park, J. S., & Hwang, J. (2003). Role-based Access Control for Collaborative Enterprise in Peer-to-Peer Computing Environments. *Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies* (pp. 93-99). Sandhu, R., Ferraiolo, D., & Kuhn, R. (2000). The NIST Model for Role-Based Access Control : Towards A Unified Standard. *Proceedings of the Fifth ACM Workshop on Role-based Access Control* (pp. 111-119). Sloman, M., Mazumdar, S., & Lupu, E. (1999). Push vs. Pull in Web-Based Network Management. *Proceedings of Sixth IFIP/IEEE International Symposium on Integrated Network Management* (pp. 3-18). Strembeck, M., & Neumann, G. (2004). An Integrated Approach to Engineer and Enforce Context Constraints in RBAC Environments. *ACM Transactions on Information and System Security*, 7(3), (pp. 392-427). Suriadi, S., Foo, E. & J?sang A. (2009). A user-centric federated single sign-on system. *Journal of Network and Computer Applications*, 32(2), (pp. 388-401). Tsaur W. J. and Lin Y. M. (2009). An Agent-based Single Sign-On Scheme for WebServices Environments, *Proceedings of the 2009 International Conference on Security and Management, I*, (pp. 220-226) Wu, E. H. K., Hsieh, M. I., & Lai, H. T. (2006). Low Latency and Efficient Packet Scheduling for Streaming Applications. *Computer Communications*, 29(9), (pp. 1413-1421). Zhang, G., & Parashar, M. (2003). Dynamic Context-aware Access Control for Grid Applications. *Proceedings of the Fourth International Workshop on Grid Computing* (pp. 101-108). Zhang X., Oh S. & Sandhu R. (2003). PBDM: A Flexible Delegation Model in RBAC. *Association for Computing Machinery* (pp. 149-157).